AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type, and wherein each dynamic behavior evaluation module records some execution behaviors of the code module as it is executed, wherein a plurality of different execution behaviors of the code module are recorded into a behavior signature corresponding to the code module;

a management module, wherein the management module obtains the code module, and wherein the management module evaluates the code module to determine the code module's type, and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the code module's type;

a malware behavior signature store storing at least one known malware behavior signature of a known malware;

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware; and

wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match at least one of a plurality of different subsets of execution behaviors recorded in a behavior signature of the known malware, wherein the different subsets of execution behaviors are pre-specified for the known malware.

2. (Currently Amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one behavior evaluation means, wherein each behavior evaluation means provides a virtual environment for executing a code module of a particular type, and wherein each behavior evaluation means records some execution behaviors of the code module as it is executed, wherein a plurality of different execution behaviors of the code module are recorded into a behavior signature corresponding to the code module;

a management means for obtaining the code module and determining the code module's type for the purpose of selecting a behavior evaluation means to execute the code module according to the code module's type;

a storage means for storing at least one known malware behavior signature of a known malware;

a behavior comparison means for comparing the behavior signature of the code module to the known malware behavior signatures in the storage means to determine whether the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware; and

wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match at least one of a plurality of different subsets of execution behaviors recorded in a behavior signature of the known malware, wherein the different subsets of execution behaviors are pre-specified for the known malware.

3. (Currently Amended) A method for determining whether a code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module as determined by a management module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording a plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module during execution of the code module;

comparing the recorded plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to a plurality of different execution behaviors of a behavior signature of a known malware;

according to the results of the previous comparison, determining whether the code module is the known malware; and

reporting whether the code module is the known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match at least one of a [[the]] plurality of different subsets of execution behaviors of the behavior signature of the known malware, wherein the different subsets of execution behaviors are pre-specified for the known malware.

4. (Currently Amended) A computer-readable storage medium storing ~~bearing~~ computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module as determined by a management module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording a plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module as the code module is executing;

comparing the plurality of different recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to a plurality of different execution behaviors of a behavior signature of a known malware;

according to the results of the previous comparison, determining whether the code module is the known malware; and

reporting whether the code module is the known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match at least one of a [[the]] plurality of different subsets of execution behaviors of the behavior signature of the known malware, wherein the different subsets of execution behaviors are pre-specified for the known malware.

5. (Previously Presented) The malware detection system of Claim 1, wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

6. (Previously Presented) The malware detection system of Claim 5, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

7. (Previously Presented) The malware detection system of Claim 6, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

8. (Previously Presented) The malware detection system of Claim 2, wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

9. (Previously Presented) The malware detection system of Claim 8, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

10. (Previously Presented) The malware detection system of Claim 9, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

11. (Previously Presented) The method of Claim 3, wherein recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

12. (Previously Presented) The method of Claim 11, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

13. (Previously Presented) The method of Claim 12, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

14. (Currently Amended) The computer-readable storage medium of Claim 4, wherein recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

15. (Currently Amended) The computer-readable storage medium of Claim 14, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

16. (Currently Amended) The computer-readable storage medium of Claim 14, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

17. (Previously Presented) The malware detection system of Claim 1, wherein the malware detection system is further configured to report a positive identification of a known malware.

18. (Previously Presented) The malware detection system of Claim 2, wherein the malware detection system is further configured to report a positive identification of a known malware.

19. (Previously Presented) The method of Claim 3, wherein reporting whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware comprises reporting a positive identification of a known malware.

20. (Currently Amended) The computer-readable storage medium of Claim 4, wherein reporting whether the code module is malware based at least in part on the degree that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware comprises reporting a positive identification of a known malware.